

初探我國金融業強化數位韌性 之法制架構

謝尚廷*

蕭惟文**

莊弘鈺***

壹、前言

隨著5G技術、雲端運算、人工智慧、物聯網等科技發展逐漸成熟普及，各組織及企業紛紛推動數位轉型，2020年新冠肺炎（covid-19）疫情爆發，更促使經濟活動從實體轉為線上化、遠距化，加速各組織及企業的數位轉型步調¹，而金融業亦受到此一數位化浪潮影響，紛紛投入數位轉型²。然而，伴隨數位轉型而來的，是資安風險對於組織及企業營運所帶來的衝擊³，而金融業擁有高價值的金融數據及資產，使其更容易成為資安攻擊的對

象，國際上金融機構遭駭事件也時有耳聞⁴。因此，對於金融業者而言，如何在推動數位轉型之際，妥適應對隨之而來的資安風險，乃其業務經營的一大挑戰。

此外，由於國家民生經濟發展有賴於金融體系之正常運作，倘若金融服務不慎中斷，小則影響民眾生活的便利，大則影響國家整體金融及經濟秩序。因此，對於國家而言，金融體系具有關鍵基礎設施（critical infrastructure）之特性，乃國家亟欲保護之對象。而各國政府為確保金融體系之穩定，亦紛紛制定各種加強金融業資安防護的政策及措施⁵，我國金融監督管理委員會（下稱金管

* 本文作者係凱基證券股份有限公司理財顧問部專家團隊組，曾任執業律師。

** 本文作者係謙眾國際法律事務所律師

*** 本文作者係國立政治大學商學院科技管理與智慧財產研究所副教授

（本文為作者於國立政治大學就讀與任教期間之研究成果，不代表任職單位立場）

（本文屬於國立政治大學「金融AI雲生態系概念驗證委託研究案」合規法遵組之部份研究成果，作者感謝澳洲蒙納許大學法學院臧正運副教授的指教與建議。）

註1：汪震亞（2022），〈數位轉型趨勢下開發中國家經濟發展的挑戰與機會〉，《經濟研究》，22期，第3頁。

註2：金融監督管理委員會（2022），《金融資安行動方案2.0》，第4頁。

註3：數位發展部（2023），《111年度國家資通安全情勢報告》，第5-8頁。

註4：金融監督管理委員會，前揭註2，第2-5頁；金融監督管理委員會（2020），《金融資安行動方案》，第2-4頁。

註5：金融監督管理委員會，前揭註2，第5-11頁。

會)亦於2020年8月、2022年12月分別推出「金融資安行動方案1.0」⁶、「金融資安行動方案2.0」⁷，並陸續推動一系列修法，從政策面及法制面加強要求我國金融業者之資通安全，以強化整體金融業之數位韌性(digital resilience)⁸。

準此，強化金融業數位韌性之法制設計可從二層面探討，一為從國家層面著手，以保護關鍵基礎設施之資通系統安全為核心；二為從產業層面著手，以確保各金融業者之資通系統具備對抗惡意攻擊或突發事件之韌性。實則，此二者的資安法制架構具有相似性，即均可將其規範內容區分為：配置資安人員、擬定資安計畫、建立資安事件通報流程等三大要求。相對來說，二者間亦有諸多不同之處，即除了兩者規範內容之詳盡程度有所差異外，前者因涉及國家及社會法益甚鉅，另定有刑罰規定，後者之規範內容不僅處理傳統資安風險⁹，更包含其他可能導致服務中斷之事件¹⁰，並要求各業者應建立營運持續管理相關措施。

本文依上述我國金融業強化數位韌性之法

制架構，區分為三個部份：一為關鍵基礎設施之資通系統保護規範；二為金融業之資通安全管理規範；三為金融業之作業韌性及營運持續管理規範。本文預計就此三部份分別進行探討，並於文末就此法制架構之發展提出建議。

貳、關鍵基礎設施之資通系統保護規範

一、金融業與國家關鍵基礎設施

金融乃屬我國八大關鍵基礎設施的主領域之一。所謂關鍵基礎設施，係指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞者¹¹。據此，關鍵基礎設施的提供者不僅有政府機關，亦包含所提供之服務對於國家社會或民生經濟有重大影響的民間機構。行政院公布之「國家關鍵基礎設施安全防護指導綱要」，即明定我國的關鍵基礎設施涵蓋八大主領域¹²，而因金融涉及國家金融秩序及民

註6：金融監督管理委員會，《金融資安行動方案》，前揭註4。

註7：金融監督管理委員會，前揭註2。

註8：所謂數位韌性，係指讓數位系統能適應變動環境，包含能從惡意的攻擊、事故，或自然發生的威脅或事件中能承受且快速恢復的能力。參國家資通安全研究院網站，數位韌性教材，https://www.nics.nat.gov.tw/core_business/digital_resilience/Digital_Resilience_Materials/（最後瀏覽日：2025年1月22日）。

註9：資安風險係指其資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以致損害其機密性、完整性及可用性，參資通安全管理法第3條第3款。常見的資安事件包含駭客攻擊、系統存取權限外洩等，參簡宏偉（2024），〈數位韌性與資安治理〉，彭芸、葉志良（編著），《數位治理：韌性·AI·規管》，第14、16頁，翰蘆。

註10：例如遭遇重大天災導致機房或營業場所受損、全球爆發重大疫情導致封城而無法營運等。

註11：資通安全管理法第3條第7款。

註12：八大主領域分別為能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區。參行政院（2018），《國家關鍵基礎設施安全防護指導綱要》，第3頁。

生經濟發展，是以上開綱要亦將金融列為關鍵基礎設施的主領域。

且各主領域又可再依其功能業務，區分出次領域；再由各次領域中，盤點維持其重要業務功能運作所需之設施與系統¹³。以金融業而言，其次領域有銀行、證券、金融支付等，其重要業務功能設施與系統則為與資金往來、證券期貨交易及貨幣支付有關之設施與系統¹⁴，詳如下表1所述。

表1：國家關鍵基礎設施領域分類——金融

次領域	重要業務功能
銀行	提供新臺幣跨行通匯資金調撥服務、ATM存提款、轉帳及餘額查詢等跨行交易服務之重要設施或系統。
證券	執行全國證券、期貨市場交易及結算、交割之重要設施或系統。
金融支付	支持我國貨幣及支付之重要設施或系統。

資料來源：行政院，國家關鍵基礎設施領域分類

上開綱要雖已盤點出我國關鍵基礎設施所涉及之領域及其重要業務功能設施，但因可能有複數單位機構提供或營運同一種關鍵基礎設施，而各單位機構之屬性及其重要性恐有差異，不宜全部納管，故有另行指定哪些單位機構應作為關鍵基礎設施提供者之必要¹⁵。是以資通安全管理法對於關鍵基礎設施提供者之指定、核定及通知等程序，另定有規定¹⁶。

準此，金融業者除須擁有上揭重要業務功能設施，亦須經指定等程序，方能成為關鍵基礎設施提供者。

二、資通安全管理法與關鍵基礎設施提供者之權利義務

關鍵基礎設施對於國家社會及民生經濟之影響不亞於政府機關，然而我國制定資通安全管理法前，資通安全之相關規範並不完善，其主要問題有三¹⁷：一、適用對象較廣泛之資通安全相關法令，有刑法妨害電腦使用罪罪章、個人資料保護法等規定，然上開規定之適用或僅就實害之結果進行處罰，或其保護客體僅以個人資料為限，並非針對資通安全管理為整體考量而制定；二、針對公務機關之資通安全，雖有行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、國家資通安全通報應變作業綱要等規定，而針對非公務機關之資通安全，亦有相關規定。然而，該等規定因分散、法令位階低、規範內容不同等問題，致使各單位機構間並無共通遵循之統一標準，難以提升國家整體資安水準；三、當時的資通安全相關法令，均未以資通安全為其主要考量，亦未要求受規範對象需以風險管理為核心，建立完整資通安全維護計畫及通報應變機制。

爰此，我國於2018年制定資通安全管理法，其規範重點除要求主管機關應推動提升

註13：同前註。

註14：行政院（2023），《國家關鍵基礎設施領域分類》，第2頁。

註15：資通安全管理法第3條立法理由；資通安全管理法草案第2條說明。

註16：資通安全管理法第16條。

註17：資通安全管理法草案總說明。

資通安全之相關措施，並課予其規範對象配置適當資安人員、制定資通安全維護計畫¹⁸、建立通報應變機制等義務，詳如下表2所示。

此外，為確保有效落實規定內容，資通安全管理法對於公務機關所屬人員及特定非公務機關違反規定之情形，定有相應行政罰則¹⁹。

表2：關鍵基礎設施提供者權利義務統整表

	公務機關	特定非公務機關
規範主體	依法行使公權力之中央、地方機關（構）或公法人（不包括軍事機關及情報機關）	<ul style="list-style-type: none"> • 關鍵基礎設施提供者 • 公營事業、政府捐助之財團法人（下稱其他特定非公務機關）
配置適當資安人員	應配置資通安全長，並由機關首長指派副首長或適當人員兼任	-
制定資安維護計畫	<ul style="list-style-type: none"> • 應依所屬之資通安全責任，並綜合考量相關資通條件，訂定、修正及實施資通安全維護計畫 • 每年向上級或監督機關提出資通安全維護計畫實施情形 • 應稽核其所屬或監督機關之資通安全維護計畫實施情形；受稽核機關有缺失或待改善者，應提出改善報告 	<ul style="list-style-type: none"> • 應依所屬之資通安全責任，並綜合考量相關資通條件，訂定、修正及實施資通安全維護計畫 • 關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形；中央目的事業主管機關並應稽核其計畫之實施情形 • 中央目的事業主管機關得要求所管之其他特定非公務機關，提出資通安全維護計畫實施情形；並得稽核其計畫之實施情形 • 受稽核單位有缺失或待改善者，應提出改善報告
建立通報應變機制	<ul style="list-style-type: none"> • 應訂定因應資通安全事件之通報及應變機制 • 知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關 • 應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關 	<ul style="list-style-type: none"> • 應訂定因應資通安全事件之通報及應變機制 • 知悉資通安全事件時，應向中央目的事業主管機關通報 • 應向中央目的事業主管機關提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交主管機關 • 知悉重大資通安全事件時，主管機關或中央目的事業主管機關得採取適當且必要之因應措施，並得提供相關協助

資料來源：本文自製

註18：依資通安全管理法施行細則第6條規定，資通安全維護計畫應包含下列事項：一、核心業務及其重要性。二、資通安全政策及目標。三、資通安全推動組織。四、專責人力及經費之配置。五、公務機關資通安全長之配置。六、資通系統及資訊之盤點，並標示核心資通系統及相關資產。七、資通安全風險評估。八、資通安全防護及控制措施。九、資通安全事件通報、應變及演練相關機制。十、資通安全情資之評估及因應機制。十一、資通系統或服務委外辦理之管理措施。十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。

註19：資通安全管理法第19至21條。

三、保護關鍵基礎設施之加重刑責規定

除訂定資通安全管理法，為提升對國家關鍵基礎設施及其他重要設施的防護，以維護社會安定及國家安全，行政院前邀集經濟部、交通部、衛生福利部、數位發展部、金管會、國家科學及技術委員會、國家通訊傳播委員會及行政院原子能委員會等8個部會，共同討論保護關鍵基礎設施之修法草案²⁰。最終決定採取統一立法原則及模式，並由各部會於其各自主管之作用法中，針對以下二行為明定特別罰則²¹：一為以竊取、毀壞等非法手段，危害該關鍵基礎設施之實體設備正常運作；二為以妨害電腦使用方式（例如破解電腦保護措施等），危害該關鍵基礎設施之核心資通系統功能正常運作。經各部會盤點後，須修正法令共計22部²²，其中與金融業相關之修法為銀行法第125條之7、第125條之8，證券交易法第174條之3、第174條之4，期貨交易法第112條之1、第112條之2。而前揭規定之保護客體，分別為財金資訊股份有限公司（下稱財金公司）、臺灣證券交易所股份有限公司（下稱證交所）、財團

法人中華民國證券櫃檯買賣中心（下稱櫃買中心）、臺灣集中保管結算所股份有限公司（下稱集保結算所）及臺灣期貨交易所股份有限公司（下稱期交所）。

四、小結

雖然資通安全管理法已明定提升公務機關及特定非公務機關資通安全之具體作法，且銀行法、證券交易法及期貨交易法亦新增保護關鍵基礎設施之加重刑責規定，以嚇阻影響金融關鍵基礎設施資通安全之外部威脅。然而，上開規定對於提升金融業整體資安之助益仍十分有限，其理由有三：一、資通安全管理法所適用之對象，僅限於經核定為關鍵基礎設施提供者之單位機構²³，其他金融業者並無上開規定之適用；二、保護關鍵基礎設施之加重刑責規定，其保護客體僅為證交所、期交所、櫃買中心、集保結算所（即金融F4）與財金公司，其他金融業者縱被指定為關鍵基礎設施提供者，亦無法受到上開規定之保護；三、資通安全管理法並未要求特定非公務機關應配置資通安全長或其他適

註20：行政院（2023），〈提升國家關鍵基礎設施及其他重大設施防護政院通過「電業法」等22項涉及保護關鍵基礎設施加重刑責之修正草案〉，<https://www.ey.gov.tw/Page/9277F759E41CCD91/d51b5370-ffa9-44fa-9715-d7d0ebbb9401>（最後瀏覽日：2025年1月22日）。

註21：同前註。

註22：電業法、天然氣事業法、石油管理法、水利法、自來水法、產業創新條例、民用航空法、商港法、氣象法、鐵路法、大眾捷運法、公路法、郵政法、醫療法、全民健康保險法、傳染病防治法、太空發展法、銀行法、證券交易法、期貨交易法、電信管理法、核子事故緊急應變法等22部法律。

註23：此外，因關鍵基礎設施提供者經中央目的事業主管機關指定，並報請主管機關核定後，係直接以書面通知該受核定者，是以外界無法得知關鍵基礎設施提供者之名單。參資通安全管理法第16條第1項；黃彥棻（2023），〈資安法實施五年首度大修法！主管機關啟動資安法修法程序〉，《iThome》，<https://www.ithome.com.tw/news/159729>（最後瀏覽日：2025年1月22日）。

當之資安人員，使特定非公務機關於資安風險治理上留有缺口²⁴。而此些問題之改善方式，除修訂資通安全管理法外²⁵，仍是有賴金管會於其職權範圍內，制定相關法令，敦促金融業者採取強化資通安全之相關措施。

參、金融業之資通安全管理規範

金管會為提升金融業的資通安全，陸續制定諸多資安相關法令及規範，而相關規定內容，似可對應至資通安全管理法所規定提升資通安全之應採取措施，包含配置適當資安人員、制定資安維護計畫及建立通報應變機制等。

一、要求金融業者配置資安長及適當資安人員

金管會自2021年9月開始，陸續修訂金融控股公司及銀行業內部控制及稽核制度實施辦法第38條之1、證券暨期貨市場各服務事業建立內部控制制度處理準則第36條之2、保險業內部控制及稽核制度實施辦法第6條之1等規定，並發布相關函令²⁶，要求金融業者應配置適當資安人員，且符合一定條件之業者，應設置資安專責單位，並指派副總經理以上或職責相當之人擔任資訊安全長，詳如下表3所示。此外，上開規定亦要求金融業者之資安人員及其他有關部門人員應接受一定時數之教育訓練，以確保員工具備落實資安防護所需的知識。

表3：金融各業資安人員配置要求

	銀行業	證券業	期貨業	投信投顧業	保險業
資安專責單位 或 資安人員	均須設置	實收資本額達200億元以上應設置； 未達200億元者，應依函令規定配置資安人員 ²⁷			均須設置
獨立 資安專責單位	資產總額達1兆元以上者，應設置	-			資產總額達1兆元以上者，應設置
資訊 安全長	均須設置	實收資本額達40億元以上或電子下單達一定比率	實收資本額達10億元以上，且電子下單達一定比率	前一年度月平均境內外管理資產規模達5000億元以上	資產總額達1兆元以上

資料來源：本文自製

註24：關於資通（訊）安全長之定義、主要職責及配置必要性，參余啟民（2023），〈資訊安全長之設置與責任初探〉，《華岡法粹》，74期，第10-13頁。

註25：行政院（2024），〈政院通過「資通安全管理法」修正草案強化國家整體資通安全法律規範、促進政府跨機關合作及區域聯防〉，

<https://www.ey.gov.tw/Page/9277F759E41CCD91/9c1b42cb-ebb2-4647-b2d6-2431ff1dfcb1>（最後瀏覽日：2025年1月22日）。

註26：金管會113年1月4日金管證券字第1120385996號令。

註27：同前註。

二、要求制定及落實資訊安全管理及評估規範

為強化金融業者之資訊安全防護能力，金融各業內部控制及稽核制度相關規定，要求各金融業者應擬定資訊安全防護機制，包含應制訂作業控管規範、緊急應變措施等²⁸，並要求各金融業者每年應針對前一年度資訊安全整體執行情形，由資訊安全長或資訊安全單位主管聯名出具內部控制制度聲明書²⁹，以示負責。此外，金融各業內部控制及稽核制度相關規定，亦授權金融各業同業公會應制定並定期檢討資訊安全自律規範³⁰。據此，金融各業同業公會亦針對各業別之需求及特性，制定相應之資訊安全自律規範，而該等自律規範之內容大致可再分為資通安全防護制度、資通安全評估及查核制度、其他因應不同服務類型及供應鏈資通安全風險等規範（詳如附錄1所示）。

上開自律規範內容，關於資通安全防護制度部分，其內容包含對於核心資通系統之明

確定義，以及金融業者對於其人員、資通系統、營運環境、個人及機敏資料等事項應採行之具體管理措施，並要求金融業者應落實營運持續管理（容後第肆部份詳述）。關於資通安全評估及查核制度部分，銀行及保險業之監管主要係委由業者自行落實及改善資訊安全相關控管措施，其資訊安全評估則可自行或委請外部專業機構辦理³¹，而各電腦系統之資訊安全評估頻率，依其重要性分類有所不同³²。與之相較，證券、期貨及投信投顧業之監管則係由證交所或期交所定期進行查核，以確認業者之資通安全控管措施是否落實且符合相關規定之要求，若有缺失，證交所或期交所並可依其營業細則或業務規則作出處分³³，其監管力度更加強烈。關於因應不同服務類型及供應鏈資通安全風險部分，則係針對業者所提供之金融數位服務，以及其所使用之新興科技，制定更為詳盡之資訊安全控管措施；又為因應金融業者與外部機構合作可能遭受跳板攻擊之風險日趨升

註28：例如金融控股公司及銀行業內部控制及稽核制度實施辦法第38條規定銀行業之風險控管機制應包含對業務或交易、資訊交互運用等建立資訊安全防護機制及緊急應變計畫；證券暨期貨市場各服務事業建立內部控制制度處理準則第10條、保險業內部控制及稽核制度實施辦法第6條均規定業者使用電腦化資訊系統應制定相應作業控管規範。

註29：金融控股公司及銀行業內部控制及稽核制度實施辦法第38條之1第3項、證券暨期貨市場各服務事業建立內部控制制度處理準則第36條之2第3項、保險業內部控制及稽核制度實施辦法第6條第3項等規定。

註30：金融控股公司及銀行業內部控制及稽核制度實施辦法第38條之1第5項、證券暨期貨市場各服務事業建立內部控制制度處理準則第36條之2第5項、保險業內部控制及稽核制度實施辦法第6條第2項等規定。

註31：金融機構辦理電腦系統資訊安全評估辦法第7條第1項。

註32：第一類電腦系統須每年至少辦理一次資訊安全評估作業，第二類電腦系統須每三年至少辦理一次資訊安全評估作業，第三類電腦系統則須每五年至少辦理一次資訊安全評估作業。金融機構辦理電腦系統資訊安全評估辦法第4條第1項。

註33：臺灣證券交易所股份有限公司營業細則第135條第2項、第144條、臺灣期貨交易所股份有限公司業務規則第126條第3款、第127條第1項第3款、第128條第1項第4款、第134條第1項。

高，相關規範亦要求金融業者與外部機構合作時應審慎評估，且應確保該外部機構符合一定之資訊安全標準，並規定雙方應明確約定之權利義務³⁴。

三、要求金融業者即時通報資安事件

為使主管機關及相關單位有效掌握金融業者發生之資通安全事件相關資訊，金管會訂定之重大偶發事件通報相關規定³⁵，即要求金融業者於發生資通安全事件，且該事件造成客戶權益受損或影響機構健全營運時，應於確認事件發生後30分鐘內，依規定以電話或通報系統將相關情事通報予各該主管機關或相關單位，並依規定辦理後續通報流程。此外，相關規定更進一步要求銀行、保險、證券及期貨業者，應於內稽內控制度中納入事件發生之通報及處理流程，並應於重大資安事件發生並通報該事件之次日起7個營業日內，依規定向主管機關或相關單位函報調查內容、處理方式及改善措施等詳細資料，以及後續處理情形。

四、小結

金融業之資通安全管理相關規範，實係分散規定於金融各業之法令及規範中，惟其規範內容架構與資通安全管理法相似，可歸納為配置資安人員、擬定資安計畫、建立事件通報流程等三大要求。然而，資通安全管理法之規定並未要求金融業者應配置資安人

員，針對資通安全維護計畫亦僅臚列計畫內容應包含之事項，對於單位組織可能面臨之資安風險及因應措施並未有更詳細之說明或規範。相形之下，金融業之規範則更為嚴謹、具體，不僅要求符合一定規模之金融業者需配置資安人員，針對營運各構面可能面臨之資安風險，亦明定業者應採行之預防及因應措施，且對於業者於資安事件發生之通報時限、流程及後續處理方式亦有具體之規定，洵有助於金融業者制定完整詳盡之資通安全管理措施。但因金融業之相關規範內容十分繁瑣，且散落於不同法令及規範，此恐增加金融業者之法令遵循難度。

肆、金融業之作業韌性及營運持續管理規範

資通系統安全對於金融業之重要性，除了在於防免客戶及業務資訊遭受外洩，更係為確保業者之營運、金融業務及資訊服務均能順利運作。然而，可能導致營運業務及資訊服務中斷的風險，不僅有資安事件，尚包含天然災害及人為災害等事由，而近來傳染性疾病大流行、氣候變遷災害加劇、地緣政治衝突風險昇高等因素，更也使業者面臨更加嚴峻的經營挑戰。因此，過往單從技術層面應對資安風險之處理方式，已無法滿足金融業資通系統所面臨之多元風險，業者必須從經營管理及風險治理等角度，擬定妥適之因

註34：謝尚廷、蕭惟文、莊弘鈺（2024），〈淺談金融業上雲趨勢與政策法令之發展〉，《萬國法律》，253期，第8-10頁。

註35：金融機構通報重大偶發事件之範圍申報程序及其他應遵循事項、保險業通報重大偶發事件之範圍申報程序及其他應遵循事項、證券期貨市場資通安全事件通報應變作業注意事項、證券商通報重大偶發事件應遵循事項、期貨商通報重大偶發事件應遵循事項。

應措施。而作業韌性及營運持續管理等概念，即在此情境需求中應運而生³⁶。

一、作業韌性與營運持續管理之濫觴及於金融業之應用

作業韌性 (operational resilience) 之概念為組織必然會遭遇衝擊營運的事件，因此組織須培養事件發生時保持應變彈性的能力，以利組織承受該不利事件所造成的衝擊，抑或減少事件所帶來的不利後果，並於事件發生後得以回復至正常營運。為達到上述作業韌性之目標，則須借助營運持續管理 (business continuity management, BCM) 措施³⁷，其概念思維係將組織面對風險之過程區分為四階段³⁸：事前預防與準備階段、緊急應變階段、業務持續階段、復原至正常運作階段。而為確保組織能順利度過各階段，組織應於事前預防與準備階段，即先釐清其核心業務，並辨識該核心業務所面臨之風險，並應進行營運衝擊分析，以理解該風險發生時對於組織營運所造成之衝擊；同時，組織應設

定各營運持續管理目標，例如最小可接受服務水準、最大可容忍中斷時間、復原時間目標、資料回復時點目標等；再者，組織應依前述目標，分別擬定緊急應對風險事件之計畫、達到營運持續之計畫以及核心業務復原之計畫；最後，為確保上開計畫均能有效落實，組織應定期執行測試和演練，並針對其結果進行檢討及改善³⁹。

關於作業韌性及營運持續管理等概念導入金融業，應可追溯至美國911事件。911事件發生時，對於美國金融體系造成莫大衝擊，其行政部門及金融業者意識到應加強金融體系面對突發事件之韌性，且因金融體系之運作具有其網絡性，若單一金融機構無法維持其作業韌性，則可能為金融體系帶來系統性風險，故金融機構應加強其短期的維持營運持續措施，並應發展長期的業務恢復計畫⁴⁰。為此，行政部門發布「增強美國金融體系韌性的健全做法跨機構文件」(Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System)⁴¹。此

註36：資誠 (PwC) 於其「韌性革命：2023全球危機與韌性調查報告」亦強調欲建立具韌性的組織，應建構作業韌性。See PwC, *The Resilience Revolution is Here: PwC's Global Crisis and Resilience Survey 2023*, PWC, 5, 9 (2023), <https://www.pwc.com/gx/en/crisis/pwc-global-crisis-resilience-survey-2023.pdf>.

註37：Richard McGlave, *Operational Resilience vs. Business Continuity*, CONTINUITY2 (Feb. 22, 2023), <https://continuity2.com/blog/operational-resilience-vs-business-continuity>; Viktorija Goryte & Stéphane Speich, *Business Continuity vs. Operational Resilience*, BCI (Nov. 15, 2022), <https://www.thebci.org/news/business-continuity-vs-operational-resilience.html>.

註38：簡宏偉，前揭註9，第17-18頁。

註39：同前註，第18-22頁。

註40：BD. OF GOVERNORS OF THE FED. RESERVE SYS., OFFICE OF THE COMPTROLLER OF THE CURRENCY & SEC. & EXCH. COMMN, INTERAGENCY PAPER ON SOUND PRACTICES TO STRENGTHEN THE RESILIENCE OF THE U.S. FINANCIAL SYSTEM, 5 (2003), <https://www.federalreserve.gov/boarddocs/press/bcreg/2003/20030408/attachment.pdf>.

註41：Id. 該文件指出營運持續的三個目標：一、面對大規模營運中斷，核心業務能迅速恢復；二、面對

後，為加強金融機構之作業韌性及營運持續管理，行政部門亦發布諸多文件⁴²，俾供業者參考、遵循，而其近期發布的「加強作業韌性的健全做法」(Sound Practices to Strengthen Operational Resilience)⁴³，旨在協助企業應對不可預見的風險，其內容彙整現有處理營運風險管理、營運持續管理、第三方風險管理、網路風險管理等議題之法規、指令、聲明和常見產業標準，讓企業可透過單一文件，掌握作業韌性及營運持續管理等各議題及規範之重點，以作為其強化作業韌性之參考依據⁴⁴。而在美國將作業韌性及營運持續管理等概念應用於金融業後，各國政府及國際組織亦紛紛效法，制定相關法令及

規範，要求金融業者建立及落實營運持續管理制度，附此敘明⁴⁵。

二、我國金融業之作業韌性及營運持續管理法令

順應國際趨勢，我國金管會亦於「金融資安行動方案1.0」、「金融資安行動方案2.0」，言明欲推動精實金融韌性，將作業韌性、營運持續管理等概念導入金融業資通安全防護體系⁴⁶，而相關規定則係制定於各金融法令及規範內。具體而言，金融各業之內部控制與稽核制度相關法令要求業者應針對資訊系統之突發狀況，制定緊急應變及系統復原等計畫⁴⁷，此即屬營運持續管理之環

失去至少一個主要業務地點或人員無法進入該地點之情形，核心業務能迅速恢復；三、通過持續使用或穩健性測試，確保關鍵的內外部持續性安排是有效且相容的。Id. at 5-6. 根據上述目標，該文件並制定四大健全做法，包含：一、識別維持重要金融市場之結算和清算活動；二、確認該結算和清算活動之適當復原目標；三、維持資源的地理分散性，以實現復原目標；四、定期使用或測試復原計畫。Id. at 8-12.

註42：例如美國聯邦金融機構檢查委員會(Federal Financial Institutions Examination Council, FFIEC)發布「資訊科技檢查手冊——營運持續管理」(Information Technology Examination Handbook booklet-Business Continuity Management)、「大流行病規劃跨機構聲明」(Interagency Statement on Pandemic Planning)等文件。BD. OF GOVERNORS OF THE FED. RESERVE SYS., OFFICE OF THE COMPTROLLER OF THE CURRENCY & FED. DEPOSIT INS. CORP., SOUND PRACTICES TO STRENGTHEN OPERATIONAL RESILIENCE 7, footnote 23 (2020), <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf>.

註43：Id. at 1.

註44：Id. 惟該健全做法主要係提供美國最大最複雜公司所使用，平均合併資產總額大於或等於(a) 2500億美元，或(b) 1000億美元且平均跨司法管轄區活動(average cross-jurisdictional activity)、平均加權短期批發性融資(average weighted short-term wholesale funding)、平均非銀行資產或平均資產負債表外風險(average off-balance-sheet exposure)為750億美元或以上的獨立國民銀行、州成員銀行、州非成員銀行、儲蓄協會、美國銀行控股公司以及儲蓄貸款控股公司。Id.

註45：金融監督管理委員會，前揭註1，第8-10頁。

註46：金融監督管理委員會，前揭註2，第30-32頁；金融監督管理委員會，《金融資安行動方案》，前揭註4，第19-20頁。

註47：金融控股公司及銀行業內部控制及稽核制度實施辦法第38條第5款規定銀行業之風險控管機制應包含對業務或交易、資訊交互運用等建立緊急應變計畫，證券暨期貨市場各服務事業建立內部控制制

節。再者，除保險業以外，金融各業的資通安全管理相關規範，則更具體地載明營運持續管理應具備之事項及要求，包含應進行營運衝擊分析、建立必要備援機制、建立對於重大資訊系統事件或天災之應變程序、定期進行營運持續性控制措施之驗證及演練等⁴⁸。

此外，金管會更敦促金融各業同業公會，應依其業別之特性，制定作業韌性參考規範，是以中華民國產物保險商業同業公會、中華民國人壽保險商業同業公會共同於2022年7月針對保險業制定「保險業資訊作業韌性參考原則」；證交所於同年8月訂定「證券暨期貨市場各服務事業資訊作業韌性參考指引」，而中華民國證券商業同業公會（下稱證券公會）、中華民國期貨業商業同業公會（下稱期貨公會）、中華民國證券投資信託暨顧問商業同業公會（下稱投信投顧公會）也於2023年8月分別針對各業別訂定「中華民國證券商業同業公會資訊作業韌性自律規範」、「中華民國期貨業商業同業公會『資

訊作業韌性自律規範』」、「證券投資信託事業證券投資顧問事業資訊作業韌性自律規範」；中華民國銀行商業同業公會全國聯合會則係於2024年3月制定「金融機構資訊作業韌性規範」。上開規範針對營業持續管理流程，有關核心業務之識別、最大可容忍中斷時間之設定、災害應變之運作機制、核心系統之復原程序、復原能力之實證等事項，有更為具體之要求。而針對符合一定條件之證券、期貨及投信投顧業者，上開規範更要求其應導入國際營運持續管理標準。

最後，為鼓勵金融業者重視其營運持續管理及作業韌性能力，證券、期貨及投信投顧公會亦分別於其公司治理實務守則中，明訂業者應定期評估其營運持續及作業韌性能力，採取適當措施，並將結果提報董事會⁴⁹。而保險業之公司治理實務守則雖未有營運持續管理及作業韌性相關規定，但其「保險業風險管理實務守則」第5.4.2點第11項，亦要求公司應依自身業務之性質、規模及複雜性，訂定適當之營運持續管理機制⁵⁰。

度處理準則第10條第9款、保險業內部控制及稽核制度實施辦法第6條第1項第11款則規定業者使用電腦化資訊系統應制定系統復原計畫及測試程序等控制作業。

註48：金融機構資通安全防護基準第17條、證券暨期貨市場各服務事業資通系統安全防護基準參考指引第12至13條、中華民國證券商業同公會資通系統安全防護基準自律規範第5條、中華民國期貨業商業同業公會資通系統安全防護基準自律規範第5條、證券投資信託事業證券投資顧問事業資通系統安全防護基準自律規範第5條、建立證券商資通安全檢查機制第10點、建立期貨商資通安全檢查機制第10點。

註49：證券商公司治理實務守則第3條之4第2款、第27條第1項第2款、期貨商公司治理實務守則第3條之4第2款、第27條第1項第2款、中華民國證券投資信託暨顧問商業同業公會證券投資信託事業證券投資顧問事業公司治理實務守則第3條之4第2款、第33條第2項第2款。

註50：有關建立營運持續管理機制之具體方式，於「保險業風險管理實務守則問答手冊」問題第5.19之回覆中，提及業者可參考美國聯邦金融機構檢查委員會（FFIEC）所發布之檢查手冊，並提供可參酌之訂定步驟，包含發展營運衝擊分析、辨識風險及評估風險事件導致業務中斷之可能性及影響程度、考量公司之經營策略及營運目標後，訂定適當之營運中斷復原目標、發展營運持續策略並建立營運持續計畫、舉辦人員教育訓練、執行演練與測試、定期檢視計畫與更新、針對機制進行監控與報告，藉此保障員工、客戶的權益及公司產品與服務。

三、小結

從作業韌性與營運持續管理之探討，可發現兩者為不同之概念，作業韌性係指組織之制度設計使其善於面對突發事件，而營運持續管理乃組織從突發事件中維持及回復核心業務運作之具體方式，是以美國制定之作業韌性相關規範，僅將營運持續管理列為提升金融業者作業韌性的方式之一，業者尚須考量其他風險因素，並採取風險控管或因應措施，方能完整建構組織整體之作業韌性。再者，美國對於作業韌性與營運持續管理等概念之應用並未限於資通安全領域，而係擴及組織整體之營運。對比之下，我國金融業之法令及規範似將作業韌性與營運持續管理視為同一概念，且相關規範之內容大多側重於業者從突發事件中回復其核心業務及資通系統之運作，至於建構組織整體作業韌性之目標，則有賴於其他內部控制及稽核制度及風險治理措施。由此可見，我國金融業應用營運持續管理與作業韌性之方式，相較於國外仍是有其特殊之處。

伍、展望代結論

為強化資通安全，我國先前制定資通安全管理法，然該法律僅適用於公務機關及特定非公務機關，雖然部分金融業者可能被指定

為特定非公務機關，而須適用該法，然該法對於提升整體金融業的資通安全助益較少。近年來，金管會留意到金融業的資安問題，故制定一系列政策及法令，且與資通安全管理法或其相關子法相比，金融業之資通安全管理、作業韌性及營運持續管理相關規範更為具體明確，且其要求亦更為嚴格，應有助於提升金融業者之資安防護能力。近期金管會檢查局亦將資通安全、營運持續管理等項目列為金融檢查重點⁵¹，亦可見金管會對於資通安全之重視。

然而，我國金融業之資通安全管理、作業韌性及營運持續管理相關規定，四散於眾多繁瑣且不同位階之法令及規範中，此種缺乏體系化之法制模式及架構，恐會增加金融業者之法令遵循難度。職是，若可參考美國作法，將散落各處之風險治理及資通安全議題加以彙整，並制定於同一規範中，應能更清晰地勾勒提升作業韌性所應採取之措施，且能避免重複規定之情形發生。又未來更應思考的是，我國金融業雖已訂有繁複詳盡之資通安全相關法令及規範，但業者是否確能落實該等法令及規範之要求，以降低資安事件發生的頻率，或減少資安事件所生的損害？此仍有待未來進一步觀察、分析，以確認我國金融業強化數位韌性之資安法制架構是否已臻完善。

（投稿日期：2025年2月5日）

註51：金融監督管理委員會檢查局，年度金融檢查重點，113年度金融檢查重點，2023年12月19日，https://www.feb.gov.tw/ch/home.jsp?id=65&parentpath=0,4&mcustomize=onemessages_view.jsp&d ataserno=202312190003&dtable=Business（最後瀏覽日：2025年1月22日）；金融監督管理委員會檢查局，年度金融檢查重點，114年度金融檢查重點，2024年12月19日，https://www.feb.gov.tw/ch/home.jsp?id=65&parentpath=0,4&mcustomize=onemessages_view.jsp&d ataserno=202412180001&dtable=Business（最後瀏覽日：2025年1月22日）。

附錄1：資訊安全評估及管理規範綜整

	銀行業	證券業	期貨業	投信投顧業	保險業
資通安全防護制度	金融機構資通安全防護基準、金融機構資訊系統安全基準	證券暨期貨市場各服務事業資通系統安全防護基準參考指引（證交所）、證券暨期貨市場各服務事業網路安全防護參考指引（證交所）			保險業辦理資訊安全防護自律規範
		中華民國證券商業同公會資通系統安全防護基準自律規範、中華民國證券商業同公會網路安全防護自律規範	中華民國期貨商業同公會資通系統安全防護基準自律規範、中華民國期貨商業同公會網路安全防護自律規範	證券投資信託事業證券投資顧問事業資通系統安全防護基準自律規範、證券投資信託事業證券投資顧問事業網路安全防護自律規範	
資安評估及查核制度	金融機構辦理電腦系統資訊安全評估辦法	建立證券商資通安全檢查機制（證交所）	建立期貨商資通安全檢查機制（期交所）	×	保險業電腦系統資訊安全評估作業原則
特別資安防護制度——因應不同服務類型	金融機構購用新興科技作業規範、金融機構辦理電子銀行業務安全控管作業基準、金融機構使用物聯網設備安全控管規範、金融機構提供行動裝置應用程式作業規範	證券期貨市場相關公會新興科技資通安全管控指引（證交所）			保險業運用新興科技作業原則、保險業網路電子商務身分驗證之資訊安全作業準則、保險業使用物聯網設備作業準則、保險業提供行動應用程式（App）作業原則
		中華民國證券商業同公會新興科技資通安全自律規範	中華民國期貨商業同公會新興科技資通安全自律規範	證券投資信託事業證券投資顧問事業新興科技資通安全自律規範	
特別資安防護制度——因應供應鏈風險	金融機構資通系統與服務供應鏈風險管理規範	證券暨期貨市場各服務事業資通系統與服務供應鏈風險管理參考指引（證交所）			保險業核心資通系統作業委外資安注意事項
		中華民國證券商業同公會供應鏈風險管理自律規範	中華民國期貨商業同公會供應鏈風險管理自律規範	證券投資信託事業證券投資顧問事業供應鏈風險管理自律規範	

（註：若規範未標註「證交所/期交所」，即係由該業同業公會所制定）

資料來源：本文自製